

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: February 26, 2010

Names of Companies covered by this certification:

Core Communications, Inc.
CoreTel Virginia, LLC
CoreTel New York, Inc.

Name of Signatory: Christopher Van de Verg

Title of Signatory: Corporate Secretary, General Counsel


I, Christopher Van de Verg, certify that I am an officer of Core Communications, Inc., and its affiliates CoreTel Virginia, LLC and CoreTel New York, Inc. (collectively, "Core"), and, acting as an agent of Core, that I have personal knowledge that the company has operating procedures and policies in place that are designed to ensure compliance with the Federal Communication Commission's ("Commission") CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures are designed to maintain compliance with the Commission's CPNI rules.

Core has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers during the 2009 calendar year. Core did not receive any customer complaints during the 2009 calendar year concerning the unauthorized release of CPNI.

Core has not discovered any information about the processes that pretexters are using to attempt to gain access to CPNI other than the publicly disclosed information in this docket. Core has taken several measures to safeguard CPNI, including, without limitation, implementing authentication/verification procedures and employing network security measures, such as encryption.

Signed:


Christopher Van de Verg

Date:

Feb. 26, 2010

CORE COMMUNICATIONS, INC.

STATEMENT OF CPNI OPERATING PROCEDURES

Core Communications, Inc. and its affiliates CoreTel Virginia, LLC; and CoreTel New York, Inc. provide this statement pursuant to Section 64.2009(c) of the Federal Communications Commission's ("Commission") rules, 47 C.F.R. § 64.2009(e), to summarize the operational procedures and policies in place that are designed to ensure compliance with the Commission's Customary Proprietary Network Information ("CPNI") rules. This statement applies equally to each company, which is collectively referred to herein as "Core."

Use of CPNI:

Core's policy is not to use, disclose or permit access to its customers' CPNI except as permitted without customer approval or as otherwise permitted by law, and only to the extent necessary. Specifically, Core may use CPNI to render, provide, bill and collect for the services from which the CPNI is derived. Core also will use CPNI to protect its property rights, or to protect its customers and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services. Core also may use CPNI to provide administrative services to the customer for the duration of the call, if the customer initiated the call and the customer approves of the use of such information to provide those services.

Employee Training:

Core trains its personnel regarding the confidentiality of customer information, including what information is classified as CPNI and when its employees are authorized and are not authorized to use this information. Core also trains its employees regarding the appropriate authentication methods, addressing account changes, responding to security breaches, among other measures.

Core has an express disciplinary process in place for the misuse of CPNI.

Breaches of Data Security:

Core has implemented procedures to notify the United States Secret Service and the Federal Bureau of Investigation in the event of a data breach. Unless law enforcement directs otherwise, we will notify affected customers after the expiration of the seven business day waiting period. We will maintain a record in accordance with section 64.2011(d) of any breaches discovered, notifications made to law enforcement, and notifications made to customers for at least two years.

Use of CPNI for Marketing Purposes:

To date, Core also does not use CPNI for any marketing purposes. Core does not use CPNI to market products and services to customers either within the category of services to which the customer subscribes or outside of that category. If Core later determines to use CPNI for marketing purposes, it will provide appropriate advance notification to its customers and maintain records of sales and marketing campaigns in accordance with the FCC's rules.

Safeguards to Protect CPNI:

Core directs its employees to discover activity that is indicative of pretexting and to take measures to protect against pretexting. Core authenticates all callers in accordance with the Commission's rules. Core prohibits the release of call detail information during an in-bound call.

Core does not permit online account access nor does it have any retail locations.

Core tracks complaints regarding the unauthorized use, disclosure of, or access to CPNI. Core will report all customer complaints to the Commission, breaking them down by category, and providing a summary of the complaints in its annual certification to the FCC. For the time period covered by the certification, Core did not receive any complaints regarding CPNI.

Core also has implemented network security measures. Among other measures, Core has implemented employee role-based access to CPNI such that employees have access to information on a need-to-know basis.

Core will notify customers immediately of certain account changes, including changes in the customer's address of record. Core does not permit customers to access their accounts online, and, therefore, the notification requirements regarding online account access are not applicable.